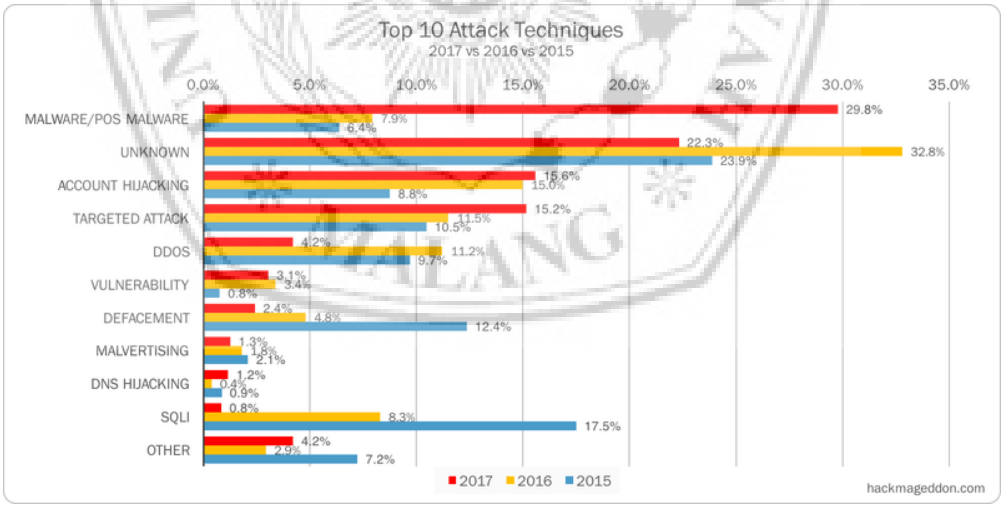
BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini semakin lama meningkat dengan pesat, ini disebabkan karena mudahnya akses informasi pada jaringan internet yang didapatkan di mana saja. Pertumbuhan pengguna internet di Indonesia dari tahun ke tahun semakin meningkat. Sebagian orang sudah mulai melupakan bahwa banyak yang telah memanfaatkan kelemahan internet untuk melakukan gangguan maupun tindak kejahatan terhadap pengguna lain. Gangguan tersebut dapat diketahui dari permasalahan-permasalahan yang telah terjadi seperti serangan *malware*, *scanning*, *brute force*, *ddos* maupun perusakan terhadap data-data pribadi yang menyebabkan kerugian besar bagi pemiliknya, dapat ditunjukkan pada **Gambar 1.1**. Menurut Anselmo Lacerda et al, telah diklasifikasikan bahwa ada lima negara peringkat dunia yang banyak melakukan serangan melalui jaringan seperti China (395 *hits*), Inggris (41 *hits*), China (39 *hits*), Perancis (23 *hits*) dan Belanda (16 *hits*) [1].



Gambar 1.1 Tren Global Teknik Serangan pada Tahun 2015 – 2017 [2]

Kurangnya pengetahuan atau informasi yang diperoleh administrator mengenai serangan *cyber* merupakan masalah yang harus diminimalisir. Untuk mengatasi masalah-masalah tersebut dibutuhkan sistem untuk mendeteksi serangan yang masuk kedalam jaringan. *Honeypot* merupakan sebuah sistem yang bekerja untuk memantau, mendeteksi serta mengumpulkan informasi penyerangan dan

sengaja dijadikan untuk tujuan diserang dan di eksploitasi [3]. *Multiple Honeypot* memungkinkan pemasangan beberapa sensor *honeypot* untuk berjalan pada satu *server*.

Secara umum, *honeypot* dibagi menjadi tiga tingkatan yaitu, *low interaction*, *medium interaction* dan *high interaction*. Semakin tinggi tingkat interaksi pada *honeypot*, maka semakin besar data yang ditangkap dan semakin besar juga resiko yang diterima [4]. Seiring dengan sulitnya menganalisis *log* yang dihasilkan oleh *honeypot*, maka dibutuhkan alat visualisasi untuk mempermudah dalam menganalisis *log honeypot*.

Pada sebelumnya untuk dapat melihat *log* yang muncul hanya berupa huruf dan angka, namun kini dengan adanya *ELK stack* untuk membaca atau melihat *log* dapat lebih mudah daripada sebelumnya. Hasil *log* pada *honeypot* divisualisasikan menggunakan *ELK stack*, di mana *ELK stack* ini adalah kombinasi *tools* berbasis *open source* yaitu *elasticsearch*, *logstash* dan *kibana* [5]. Hasil visualisasi yang tersimpan pada *ELK stack* sangat berguna bagi administrator untuk melakukan identifikasi masalah pada *server*.

Pada penelitian yang telah dilakukan sebelumnya oleh Romadhan [6] proses pengiriman *log* yaitu ketika terjadi serangan *honeypot* akan mencatat serangan tersebut dan menyimpannya di dalam *log.JSON*. Data *log* dari masing-masing *honeypot* akan dikirim menggunakan *plug in filebeat*. *Log* akan diolah *ELK server* dan kemudian akan divisualisasikan pada *web browser*. Ancaman keamanan yang dilakukan oleh *sniffer* adalah kemampuan mereka untuk menangkap semua paket yang masuk dan keluar melalui jaringan, yang meliputi kata sandi, nama pengguna dan masalah sensitif lainnya [7]. Kekurangan dari penelitian sebelumnya yaitu belum terpasang nya *private key* dan *ssl certificate* sehingga masih terdeteksi paket-paket penting yang berhubungan dengan pengiriman *log* dari sensor *honeypot* ke *ELK server*. *Private key* merupakan kunci yang digunakan untuk otentikasi pada *client*. *Secure Socket Layer* (SSL) merupakan protokol kemanan jaringan yang dikembangkan oleh *Netscape* untuk menjamin kemanan data yang ditransmisikan melalui internet [8].

Pada penelitian ini, implementasi *multiple honeypot* akan dipasang pada komputer *desktop*. Sensor-sensor *honeypot* yang akan digunakan yaitu *dionaea*, *cowrie*, dan *suricata*.

Dionaea merupakan salah satu *honeypot* dengan tingkat interaksi menengah yang digunakan untuk menjebak dan mendeteksi serangan. *Honeypot* ini juga meniru beberapa protokol seperti *FTP, HTTP, HTTPS, MySQL,* dan lain-lain [9].

Cowrie merupakan *honeypot* dengan interaksi menengah yang digunakan untuk mencatat interaksi serangan seperti *brute force* untuk menyerang ssh dan telnet [9].

Suricata merupakan perangkat lunak berbasis *open source* seperti *IDS* dan *IPS* yang berguna untuk mendeteksi dan mencegah serangan yang masuk melalui jaringan komputer [10]. Serangan-serangan yang dapat di deteksi oleh *suricata* ini yaitu seperti *port scanning* untuk mendapatkan informasi menyeluruh mengenai status *port* dan *brute force* untuk mendapatkan *user* id dan *password* yang menjadi target.

Pengiriman *log* oleh sensor-sensor *honeypot* terhadap *ELK server* akan diberikan suatu *private key* dan *ssl certificate* untuk memverifikasi identitas *ELK server* yang berfungsi untuk keamanan komunikasi antara *honeypot server* dan *ELK server*.

Berdasarkan latar belakang di atas peneliti tertarik mengangkat judul yaitu "Implementasi *Multiple Honeypot* dan Keamanan Komunikasi pada ELK *stack* Menggunakan *Ssl Certificate*".

1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan *multiple honeypot* dan visualisasi *log honeypot* pada ELK *stack*?
2. Bagaimana uji keamanan pada ELK *stack* menggunakan *ssl certificate*?

1.3 Batasan Masalah

1. Implementasi beberapa *honeypot* diantaranya *cowrie*, *dionaea*, dan *suricata*.
2. Perangkat lunak yang digunakan untuk pengujian adalah perangkat lunak berbasis *open source* yaitu *wireshark*.

3. Teknik pengujian serangan pada penelitian ini menggunakan teknik *sniffing*.

1.4 Tujuan

1. Mengetahui implementasi *multiple honeypot* dan visualisasi *log honeypot* pada ELK *stack.*
2. Mengetahui uji keamanan pada ELK *stack* menggunakan *ssl certificate*.

1.5 Manfaat

Penelitian ini diharapkan memberi manfaat antara lain:

1. Memberikan peringatan awal bagi administrator dalam menjaga, dan melakukan tindakan pencegahan serangan terhadap jaringan.
2. Membantu administrator dalam melakukan monitoring jaringan secara *real time*.
3. Memudahkan administrator untuk membaca *log* dan mengidentifikasi masalah pada *server*.
4. Keamanan komunikasi dan pengiriman data dari *honeypot server* ke ELK *server.*

1.6 Metodologi

Penelitian dilakukan dengan menggunakan beberapa metode penelitian, di antaranya:

1.6.1 Studi Pustaka

Dalam penelitian ini, penulis melakukan studi pustaka dari berbagai literatur termasuk dari buku, makalah-makalah, artikel ilmiah, jurnal, dan bahan-bahan dari internet yang sesuai dengan penelitian ini. Sumber pustaka antara lain berhubungan dengan kemanan jaringan, *dionaea honeypot, suricata honeypot, cowrie honeypot,ELK stack, dan ssl certificate*.

1.6.2 Desain Sistem (Perancangan)

Berdasarkan studi pustaka yang telah dilakukan, dapat ditentukan bagaimana desain dari sistem yang akan dibuat. Pada tahap ini, dilakukan dengan merancang desain sistem yang akan dibangun.

1.6.3 Implementasi Sistem

Pada tahap ini dilakukan implementasi sesuai dengan perancangan yang dibuat, dimulai dari instalasi perangkat lunak yang akan dipakai dan konfigurasi pada sistem yang akan dibangun.

1.6.4 Pengujian Sistem

Pengujian ini dilakukan untuk membuktikan sejauh mana kesesuaian sistem yang dibangun bekerja dengan fungsionalitas dan tujuan perancangan. Adapun beberapa rancangan pengujian didasarkan terhadap beberapa hal, antara lain apakah sistem yang dirancang mampu menangkap dan memberikan peringatan serangan, hasil yang ditangkap oleh *honeypot*, visualisasi *log* dari *honeypot* yang ditampilkan oleh *ELK stack*, dan memverifikasi identitas sensor yang mengirimkan *log* datanya menggunakan *ssl certificate*.

1.6.5 Sistematika Penelitian

Pada sistematika penulisan ini akan digambarkan secara menyeluruh permasalahan yang akan dibahas. Untuk memudahkan penulisan sistematika penulisan dibuat menjadi lima bagian, antara lain:

1. BAB I PENDAHULUAN

Bab ini mencakup latar belakang penelitian yang berjudul "*Implementasi Multiple Honeypot* dan *Keamanan Komunikasi* pada *ELK stack Menggunakan Ssl Certificate*", rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, keaslian penelitian, metode penelitan dan sistematika penulisan.

2. BAB II TINJAUAN PUSTAKA

Bab ini mencakup teori-teori, informasi, dan kajian penelitian sebelumnya yang berkaitan dengan lingkup penelitian yang dilakukan sesuai dengan literatur. Tinjauan pustaka ini akan digunakan penulis sebagai referensi dalam melakukan penelitian dan mengemukakan argumen pada hasil penelitian.

3. BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini mencakup analisis kebutuhan *hardware* dan *software* yang digunakan. Selain itu dijelaskan beberapa perancangan yang akan dibuat, perancangan tersebut meliputi rancangan sistem dan skenario pengujian.

4. BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini mencakup implementasi atau pengujian terhadap sistem dan hasil pengujian. Tahap ini dilakukan setelah sistem didesain dan dianalisis pada perancangan sistem.

5. BAB IV PENUTUP

Bab ini mencangkup kesimpulan dan saran yang bisa diambil berhubungan dengan sistem yang dibuat dan saran untuk meningkatkan sistem lebih lanjut.